AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

District of Delaware

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

3. One WD My Book Hard drive (black), currently located at New Castle County Police Dept., 3601 N. Dupont Hwy, New Castle, DE

Case No. 25- 368 M

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of Delaware, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252(a)(2), (a)(4)(b), (b)(1), (b)(2)	Distribution and possession of child pornography, and attempt

The application is based on these facts:

See Attached Affidavit of Probable Cause

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

s/ SA Brian Mitchell
Applicant's signature

FBI SA Brian Mitchell
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: 7/8/2025

Judge's signature

City and state: Wilmington, Delaware

Hon. Eleanor G. Tennyson, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A SEARCH WARRANT

I, Brian S. Mitchell, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION AND AFFIANT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search **TARGET DEVICES 1, 2, 3, 4, 5, 6, 7, 8, and 9** (further described below and in Attachment A), currently located in the New Castle County Police Headquarters at 3601 N. Dupont Highway, New Castle DE, for evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(2) and (a)(4)(b), (b)(1), (b)(2) (distribution and possession of child pornography, and attempt) (hereinafter, the "**SPECIFIED FEDERAL OFFENSES**"), more fully described in Attachment B. Attachments A and B are incorporated herein by reference. The **TARGET DEVICES** to be searched, all currently located at New Castle County Police Headquarters, are:

- Blue Motorola cellphone (cracked upper right portion of screen) – seized from JEREMIAH WALTERS ("**TARGET DEVICE 1**")
- Tablet (Painted purple back in multicolored case with name "Feddy" written on case) – seized from inside leather folder front passenger floorboard of Ford truck ("**TARGET DEVICE 2**")
- Black WD MyBook Hardrive – seized from inside backpack front passenger floorboard of Ford truck ("**TARGET DEVICE 3**")
- Black Samsung Tablet (SN: R52HA1GPF3T) – seized from inside backpack front passenger floorboard of Ford truck ("**TARGET DEVICE 4**")
- White HP Tablet (Beats label – lower right-hand corner) – seized from inside backpack front passenger floorboard of Ford truck ("**TARGET DEVICE 5**")
- Black Toshiba Laptop (SN: XE254740P) – seized from front passenger floorboard of Ford truck ("**TARGET DEVICE 6**")
- Black Toshiba Laptop (SN: 6C351646Q) – seized from under front passenger seat of Ford truck ("**TARGET DEVICE 7**")
- Black cellphone (marker on back of phone - cracked screen) – provided by WITNESS from RV ("**TARGET DEVICE 8**")
- Black Schok cellphone (cracked screen) – provided by WITNESS from RV ("**TARGET DEVICE 9**")

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since July 2017. I am currently assigned to the Baltimore Field Office of the FBI, in the Wilmington, Delaware Resident Agency. I have received specialized training in human trafficking and child exploitation investigations, computer and cell phone analysis for such investigations, search warrant writing, and the enforcement of federal laws. I have received training in child sexual abuse material and child exploitation and have had the opportunity to observe and review numerous examples of visual depictions of minors engaged in sexually explicit conduct (as defined in 18 U.S.C. § 2256), often referred to by law enforcement as child sexual abuse material.

3. I have learned about violent crimes against children through training at the FBI Academy, various conferences and trainings, and everyday work related to conducting such investigations. I am aware that those who travel in interstate commerce and use interstate facilities for the purposes of committing offenses against children commonly use electronic devices in furtherance of their illegal activities. The electronic devices are used to access the internet for communication with potential victims and storing images/videos.

4. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, including but not limited to violations of 18 U.S.C. §§ 2422, 2423, 2251, and 2252. I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

5. As set forth more fully below, I submit that there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2), (b)(1) (distribution of child pornography, including attempt) and 2252(a)(4)(B), (b)(2) and (possession

of, or access with intent to view, child pornography, including attempt) are located within the **TARGET DEVICES** which were once in the possession of **JEREMIAH WALTERS** (hereinafter, "**WALTERS**").

6. I submit this affidavit in support of an application for a search warrant authorizing a search of the **TARGET DEVICES**, as further described in Attachment A, respectively, incorporated herein by reference, and to seize evidence, fruits, and instrumentalities of the foregoing criminal violations, as more fully described in Attachment B, which is also incorporated herein by reference.

7. The facts contained in this affidavit are based in part on information and reports provided by U.S. federal law enforcement agents and state law enforcement officers; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, independent investigation and analysis by law enforcement agents/analysts and computer forensic professionals, and my experience, training, and background as a Special Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish that there is sufficient probable cause for the requested warrant. I have not, however, knowingly withheld any fact necessary to a determination of probable cause.

PROBABLE CAUSE

A. Summary

8. In September 2024, your affiant received information regarding a subject in the Newark, Delaware area who had uploaded, sent, and discussed child pornography via the social

media application Kik Messenger[1], which is owned by MediaLab. Since then, law enforcement has positively identified the Delaware subject as **WALTERS** and his residence as 61 Garden Lane, Newark DE.

9. On April 24, 2025, New Castle County Police Department (NCCPD) responded to a domestic dispute involving WALTERS and a confidential witness (WITNESS) at the above address. During the incident, the WITNESS advised she observed several videos and images consistent with what she described as "child pornography" and described some of the videos and images to NCCPD. NCCPD seized the **TARGET DEVICES** during the incident.

B. <u>NCMEC Cybertip Submission (Report: 199424940)</u>

10. On September 24, 2024, Media Lab submitted CyberTipline report (hereafter, "Cybertip") 199424940 to the National Center for Missing and Exploited Children (NCMEC)[2] to advise they had identified the Kik username, "PrettyPP09081989," who uploaded suspected files of child pornography into his or her Kik account.

11. Your affiant identified **WALTERS'** date of birth as 09-08-1989 which resembles the numerical portion of the username provided by Kik, "PrettyPP09081989".

---

[1] Kik Messenger is a free social networking service owned by MediaLab. Kik allows users to create a profile using an email address, which does not need to be verified. The users can then post and share photographs and videos with other users on the platform. Users can also send a private message to other users and also send photographs or videos directly to another user. The Kik application is primarily used on a smart device, such as an Apple iPhone, Android cell phone, Apple iPad, or Android tablet is a cloud-based communications platform that allows users to connect via video, audio, phone, and chat.

[2] NCMEC's CyberTipline is the national online clearinghouse for tips and leads about child sexual exploitation. NCMEC receives complaints via their CyberTipline from Internet Service Providers (ISPs), Electronic Service Providers (ESPs), and others. These CyberTipline reports are reviewed by a NCMEC analyst and forwarded to Law Enforcement for further investigation on the information provided in the CyberTipline report. ISPs, ESPs, and others may physically view a picture, video, or any other content that they would then report to NCMEC. ISPs and ESPs may also use systems or databases that flag files they have seen in the past that they have determined depicted minors engaged in sexually explicit conduct.

12. The Cybertip provided the incident type as "Child Pornography (possession, manufacture, and distribution)" and the incident time as 09-12-2024 at 09:15 UTC.

13. The Cybertip also provided the home email address as feddyjeddy89@gmail.com.

14. As part of the Cybertip, Kik provided three files that were uploaded into this account, along with limited subscriber and login history for the account.

15. The user logged into his or her account on September 11, 2024, from IP Address 76.98.203.86, Port: 11186, at 16:41 UTC.

16. The Cybertip indicated that personnel at Kik viewed the files of suspected child pornography before providing them to NCMEC.

17. Your Affiant reviewed these files and in your affiant's opinion, all three files are visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256. The files depict prepubescent minor girls engaging in the lascivious display of the genitals or pubic area. The files are described below to establish probable cause:

- **52ab723d-49fd-4d4f-9e10-25c32127f044.mp4** –A 28-second video depicting a prepubescent minor girl, nude from the waist down, on her hands and knees, with her vagina and anus exposed. The girl repeatedly slaps and spreads apart her buttocks with her hands.
- **e203aba3-c58b-44f3-8557-59ae5fc30214.mp4** – A 42-second video depicting a nude, prepubescent minor girl dancing around in a circle and posing for the camera while her vagina is exposed.
- **11584a6c-70dd-47b7-aeb8-5f5f13a948c5.jpg** – An image depicting a prepubescent minor girl with her underwear pulled down around her thighs, exposing her vagina and anus.

18. The files were uploaded on 09-12-2024 to Kik account "PrettyPP09081989."

19. On February 25, 2025, the FBI submitted a preservation letter to MediaLab to preserve the content associated with Kik username "PrettyPP09081989" and Cybertip 199424940.

20. On February 25, 2025, an administrative subpoena was served on Comcast for subscriber information relating to IP address 76.98.203.86, Port: 11186 on September 11, 2024, at 16:41 UTC. Comcast provided results showing this IP address was assigned to the account registered to FEDERIC WALTERS, with billing address of 61 Garden Lane, Newark, Delaware 19702.

21. On February 26, 2025, an administrative subpoena was served on Google for subscriber information relating to email address feddyjeddy89@gmail.com. Google provided results showing the email address subscriber information as "Jeremiah Walters" with the created-on date as 09-17-2011. The recovery email for the Google account was identified as feddyjeddy895010@aol.com and the recovery phone number as 1-302-665-0048.

22. Of note in relation to this phone number, on July 15, 2024, the New Castle County Police Department (NCCPD) responded to 61 Garden Lane, Newark DE in reference to a domestic dispute. During the incident, NCCPD made contact with **WALTERS**. The NCCPD Officer documented in the police report that **WALTERS** provided his phone number as 1-302-665-0048 the same number as the recovery number for the Google account feddyjeddy89@gmail.com.

C. <u>Kik Search Warrant & Return</u>

23. On March 20, 2025, your affiant obtained a search warrant from the Honorable Eleanor G. Tennyson, United States Magistrate Judge for the District of Delaware for the

account associated with the Kik username, "PrettyPP09081989" (Case No: 25-133M), and served the warrant on Kik Messenger on the same date.

24. On April 8, 2025, your affiant received the search warrant results from Kik for the username, "PrettyPP09081989".

25. Your affiant reviewed the results provided from Kik Messenger which identified several files consisting of chat conversations, chat sent files, content files containing videos and images.

26. Within the files, your affiant located the same three files described above in paragraph #16, which were all visual depictions of minors engaged in sexually explicit conduct in your affiant's opinion. The file names were identified as 11584a6c-70dd-47b7-aeb8-5f5f13a948c5, e203aba3-c58b-44f3-8557-59ae5fc30214, and 52ab723d-49fd-4d4f-9e10-25c32127f044. The files were all sent on September 12, 2024.

27. Your affiant also located additional files which were consistent with child erotica and anime within the Kik results.

28. On September 12, 2024, the below conversation occurred between Kik username, "PrettyPP09081989" and username, "Conron3533":

sender_jid	receiver_jid	chat_type	msg	sent_at
conron3533_0xd	prettypp09081989_rp4	chat	You down to trade?	2024-09-12T09:02:14Z
prettypp09081989_rp4	conron3533_0xd	chat	Sure what u got	2024-09-12T09:03:08Z
conron3533_0xd	prettypp09081989_rp4	chat	Young	2024-09-12T09:04:36Z
conron3533_0xd	prettypp09081989_rp4	chat	You?	2024-09-12T09:04:38Z
prettypp09081989_rp4	conron3533_0xd	chat	I got some lol	2024-09-12T09:04:58Z
conron3533_0xd	prettypp09081989_rp4	chat	Lets trade	2024-09-12T09:05:08Z
conron3533_0xd	prettypp09081989_rp4	chat	Iâ€™ll send 5 u send 5	2024-09-12T09:05:22Z
conron3533_0xd	prettypp09081989_rp4	chat	Any vids?	2024-09-12T09:05:48Z
conron3533_0xd	prettypp09081989_rp4	chat	Yo?	2024-09-12T09:08:00Z
prettypp09081989_rp4	conron3533_0xd	chat	Sending	2024-09-12T09:08:34Z
prettypp09081989_rp4	conron3533_0xd	chat	I wish I had more real stuff rather than hentai type stuff lol	2024-09-12T09:09:26Z
conron3533_0xd	prettypp09081989_rp4	chat	Yeah	2024-09-12T09:09:50Z
conron3533_0xd	prettypp09081989_rp4	chat	More	2024-09-12T09:29:08Z

29. Your affiant advises during the conversation, Kik username "PrettyPP09081989" discussed trading visual depictions of minors engaged in sexually explicit conduct, specifically stating "I got some lol" when responding to a question from Kik username "Conron3533" asking "You?".

30. During the same conversation, "PrettyPP09081989" sent "Conron3533" a message stating "Sending" on 09-12-2024 at 09:08.

31. When reviewing the "chat platform sent files", your affiant located files sent from Kik username "PrettyPP09081989" to "Conron3533". The files names were identical to the files identified as visual depictions of minors engaged in sexually explicit conduct described above. The file names were identified as 11584a6c-70dd-47b7-aeb8-5f5f13a948c5 sent on 09-12-2024 at 09:10, e203aba3-c58b-44f3-8557-59ae5fc30214 sent on 09/12/2024 at 09:14, and 52ab723d-49fd-4d4f-9e10-25c32127f044 sent on 09/12/2024 at 09:15.

prettypp09081989_rp4	conron3533_0xd	Gallery	11584a6c-70dd-47b7-aeb8-5f5f13a948c5	9/12/2024 9:10
prettypp09081989_rp4	conron3533_0xd	Gallery	52ab723d-49fd-4d4f-9e10-25c32127f044	9/12/2024 9:14
prettypp09081989_rp4	conron3533_0xd	Gallery	e203aba3-c58b-44f3-8557-59ae5fc30214	9/12/2024 9:15

32. Your affiant advises the files were sent from Kik username "PrettyPP0908198" to "Conron3533" a few minutes after "PrettyPP09081989" replied with "Sending". "PrettyPP09081989" sent a total of three files after replying "Sending".

33. Your affiant also located additional conversations between Kik username "PrettyPP09081989" and "Hyperowl1337" from 09/11/2024 and 09/12/2024. During the conversation, "PrettyPP09081989" stated "Mmmmm need to see more of that stuff lol need some boy stuff too lol", "Pheeewwwwww weeeeeeee I tell u what…. We would wear all them little holes out by the time we were done", "Wanna adopt like 15 of them and make them take turns sucking our cocks and eating our asses and for me personally all the little boys can take turns

getting their little hairless dicks hard enough to let them take turns putting it in my ass", followed by "Then I'd hang one of the girls by her ankles with my arms and id set her throat down onto my cock feeling her tight little esophogus [sic] stretch to fit my thick cock in her neck and i may keep her theur [sic] until she's bluish looking then id let her live barely untik [sic] next break when i destroy her fragile throat with my cock".

34. Below is an excerpt from the Kik conversation between "PrettyPP09081989" and "Hyperowl1337".

sender_jid	receiver_jid	msg	sent_at
prettypp09081989_rp4	hyperowl1337_5xz	Mmmmm need to see more of that stuff lol need some boy stuff too lol	2024-09-11T09:57:18Z
prettypp09081989_rp4	hyperowl1337_5xz	Mmmmmm fuck that's so hot ðŸ˜ðŸ˜ðŸ˜	2024-09-11T10:00:04Z
hyperowl1337_5xz	prettypp09081989_rp4	Wish there could get my hands on any of them -_-	2024-09-11T10:01:10Z
prettypp09081989_rp4	hyperowl1337_5xz	Pheeewwwwww weeeeeeee I tell u what..... We would wear all them little holes out by the time we were done	2024-09-11T10:02:25Z
hyperowl1337_5xz	prettypp09081989_rp4	Same here fren	2024-09-11T10:02:54Z
prettypp09081989_rp4	hyperowl1337_5xz	Wanna adopt like 15 of them and make them take turns sucking our cocks and eating our asses and for me personally all the little boys can take turns getting their little hairless dicks hard enough to let them take turns putting it in my ass	2024-09-11T10:05:30Z
prettypp09081989_rp4	hyperowl1337_5xz	Then I'd hang one of the girls by her ankles with my arms and id set her throat down onto my cock feeling her tight little esophogus stretch to fit my thick cock in her neck and i may keep her theur until she's bluish looking then id let her live barely untik next break when i destroy her fragile throat with my cock	2024-09-11T10:09:20Z
prettypp09081989_rp4	hyperowl1337_5xz	Please send more lol anything like that is fire	2024-09-11T10:10:29Z
prettypp09081989_rp4	hyperowl1337_5xz	Hey	2024-09-12T08:52:39Z

D. NCCPD Responds to Domestic Incident at WALTERS Residence – 04/24/2025

35. On Thursday, April 24, 2025, NCCPD Officers responded to the residence of **WALTERS** and made contact with the WITNESS in reference to a domestic dispute. NCCPD Officers interviewed the witness, which was recorded on the Officers' bodycam.

36. The WITNESS advised during the incident with **WALTERS** that she had reviewed several files, consisting of videos and images, on **WALTERS'** blue Motorola cell phone (**TARGET DEVICE 1**) which appeared to be, in her words, "child pornography."

37. The WITNESS said the images and videos were located in the "Google photos" application on **TARGET DEVICE 1** and the WITNESS observed approximately 50 files containing "child pornography" which she described as "little girls/little boys, down to infants,

getting raped."

38. The WITNESS described the videos as "naked little kids doing sexual acts" and "adults forcing kids to do sexual acts." The "kids" consisted of all different ages and the age group was wide, the WITNESS described, stating "very, very young kids."

39. The WITNESS described a video of an "adult male making a little girl put her mouth on his penis." Also observed by the WITNESS was a video of a "little girl screaming, and the guy kept shoving his dick in her mouth," as well as a video of a "woman sucking and touching a little boy's penis." The WITNESS observed pictures of nude little girls and nude little boys spreading their legs and touching each other.

40. The WITNESS was visibly upset, crying excessively, when describing the above images and videos. The WITNESS stated she had to stop viewing them and could not look at them anymore.

41. The WITNESS also stated she observed a nude picture of her friend's daughter, who was approximately 13 years old, within the "Google photos." The WITNESS explained she had previously seen the original photograph of her friend's daughter on Facebook account and believed WALTERS took the original photograph from her friend's Facebook account and utilized an "application" to alter the photograph to make the girl appear nude. The WITNESS described the image of her friend's daughter being completely nude, appearing to show her breasts and vagina.

42. The WITNESS stated **WALTERS** utilized applications on his devices including "Kik," "Snapchat," and "Reddit" to chat and share images and videos with people. The WITNESS provided **WALTERS'** email address as "feddyjeddy9889@gmail.com."

43. The WITNESS was aware **WALTERS** previously received a letter from

"Snapchat" in approximately 2022 or early 2023 stating that **WALTERS** posted inappropriate items to "Snapchat" and if the posts continued, a further investigation would be conducted.

44. The WITNESS explained **WALTERS** had two old phones, described herein as **TARGET DEVICE 8** and **TARGET DEVICE 9**, at the "RV" (recreational vehicle) the WITNESS shared with **WALTERS** located at **WALTERS'** address. The WITNESS also advised there were several electronics, including a Toshiba laptop, within **WALTERS'** pickup truck.

45. While NCCPD Officers were speaking with the WITNESS, **WALTERS** responded back to the residence and was taken into custody in reference to the domestic dispute. When taking **WALTERS** into custody, NCCPD Officers seized **WALTERS'** cell phone, **TARGET DEVICE 1**.

E. NCCPD Interview of WALTERS – 04/25/2025

46. On April 25, 2025, a post-*Miranda* interview was conducted with **WALTERS** by NCCPD. During the interview, **WALTERS** stated his current email address was feddyjeddy89@hotmail.com.

47. **WALTERS** explained he previously had "Snapchat," but the account was linked to an old phone number and also previously had a "Kik" account, however he could not recall the username or email that was associated with the "Kik" account.

48. **WALTERS** previously used "Kik" to talk to people, mostly sexual in nature, and last utilized the application a few months ago. **WALTERS** stated the "Kik" application was on his current phone, but he was not signed into the application.

49. When previously using the "Kik" application, specifically talking with people, **WALTERS** recalled nude images of children "popping up," but he would immediately delete

the image and block the person.

50. **WALTERS** said he accesses various groups on "Reddit,"named, *e.g.,* "Dirty Snapchat" and "Gay Snapchat," to meet people and will gain their Snapchat usernames, ultimately switching over to the Snapchat application to continue communicating with such individuals.

51. **WALTERS** utilizes "Snapchat" to talk to other males and uses the application primarily for sexual purposes.

52. **WALTERS** advised he has had his current cell phone, **TARGET DEVICE 1**, for approximately 3 months.

F. NCCPD Search Warrant and Seizure of TARGET DEVICES

53. On April 25, 2025, NCCPD Detective D. Diprima signed and executed a state search warrant for **WALTERS'** vehicle which was identified as a black 1993 Ford F150 pickup truck. The search warrant was signed in the State of Delaware, Justice of the Peace Court 11 by the Honorable Amanda Moyer.

54. During the search of the vehicle, NCCPD located several electronic devices within the vehicle including a Tablet with painted purple back in multicolored case with "Feddy" written on the case inside a leather folder on the front passenger floorboard (**TARGET DEVICE 2**), a black WD MyBook Hard Drive from inside a backpack on the front passenger floorboard (**TARGET DEVICE 3**), a black Samsung Tablet – SN: R52HA1GPF3T from inside a backpack on the front passenger floorboard (**TARGET DEVICE 4**), a white HP Tablet with "Beats" label in lower right hand corner from inside a backpack on the front passenger floorboard (**TARGET DEVICE 5**), a black Toshiba Laptop – SN: XE254740P from the front passenger floorboard (**TARGET DEVICE 6**), and a black Toshiba Laptop – SN: 6C351646Q from under the front

passenger seat (**TARGET DEVICE 7**).

55. The WITNESS provided NCCPD Officers two old phones, which were once possessed by **WALTERS**, consisting of a Black cellphone with marker on back of phone (**TARGET DEVICE 8**) and a Black Schok cellphone (**TARGET DEVICE 9**). The devices were located inside the WITNESS'S and **WALTERS'** "RV".

56. All the TARGET DEVICES, which were seized during the search, were entered into NCCPD evidence and are all currently being stored at NCCPD Headquarters located at 3601 N. Dupont Highway, New Castle DE.

G. Additional NCMEC Cybertip Submissions (Reports: 95489916 / 122266818 / 169072158 / 175292892)

57. Based on the above information, your affiant requested additional information/queries from NCMEC pertaining to **WALTERS'** personal information, including the email addresses "feddyjeddy89@hotmail.com" and "feddyjeddy9889@gmail.com" provided by **WALTERS** and the WITNESS to NCCPD.

58. NCMEC provided four additional CyberTipline reports including 95489916, 122266818, 169072158, and 175292892. These Cybertip reports are described serially as follows.

59. On July 16, 2021, Snapchat[3] submitted Cybertip report 95489916 to NCMEC advising they had identified the Snapchat username, "feddyjeddy89," who uploaded and/or sent suspected files of child pornography into his or her Snapchat account.

[3] Snapchat Messenger is a mobile messaging app focused on sharing photos and videos, often with the feature that they disappear after being viewed. Snapchat users can take photographs and videos, which can be sent to individual friends or saved to their story. A user's story is a collection of their snaps from the day, displayed in chronological order. Users can have one-on-one or group conversations with their friends via text and pictures.

60. The Cybertip provided the incident type as "Child Pornography (possession, manufacture, and distribution)" and the incident time as 07-15-2021 at 17:03 UTC.

61. The Cybertip also provided the email address as feddyjeddy89@hotmail.com.

62. As part of the Cybertip, Snapchat provided three files that were uploaded into this account.

63. The Cybertip indicated that the personnel at Snapchat viewed the files of suspected child pornography before providing them to NCMEC.

64. Your Affiant reviewed these files and in your affiant's opinion, the files are visual depiction of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256. The files depict prepubescent minor girls engaging in the lascivious display of the genitals or pubic area.

65. The files were uploaded on 07-15-2021 to Snapchat account "feddyjeddy89."

66. On April 15, 2022, Snapchat submitted Cybertip report 122266818 to NCMEC advising they had identified the Snapchat username, "noodsmydood," who uploaded a suspected file of child pornography into his or her Snapchat account.

67. The Cybertip provided the incident type as "Child Pornography (possession, manufacture, and distribution)" and the incident time as 04-14-2022 at 09:49 UTC.

68. The Cybertip also provided the associated email address as feddyjeddy89@hotmail.com.

69. As part of the Cybertip, Snapchat provided one file that was uploaded into this account.

70. The Cybertip indicated that the personnel at Snapchat viewed the file of suspected child pornography before providing them to NCMEC.

71. Your Affiant reviewed the file and in your affiant's opinion, the file is a visual depiction of minor engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256. The file depicts a prepubescent minor boy engaging in the lascivious display of the genitals or pubic area. The file is described below:

- **noodsmydood-None-c798dd15-e65e-58cd-a5cd-9f3c52004496-27-e5b5adc85e.mp4** –A 44-second video depicting a prepubescent minor boy, nude from the waist down, lying on his back. An adult female is observed performing oral sex on the boy. During the video, the adult female asks the child "does it tickle."

72. The file was uploaded on 04-14-2022 to Snapchat account "noodsmydood."

73. On August 4, 2023, Reddit, Inc. [4] submitted Cybertip report 169072158 to NCMEC advising they had identified the Reddit username, "Usual_Technology_645," who uploaded a suspected file of child pornography into his or her Reddit account.

74. The Cybertip provided the incident type as "Child Pornography (possession, manufacture, and distribution)" and the incident time as 08-03-2023 at 12:10 UTC.

75. The Cybertip also provided the associated email address as feddyjeddy89@hotmail.com.

76. As part of the Cybertip, Reddit provided one file that was uploaded into this account.

77. The Cybertip indicated that the personnel at Reddit viewed the file of suspected child pornography before providing them to NCMEC.

[4] Reddit, Inc, is a social news aggregation, internet forum, and social media platform where users can submit content like links, text posts, images, and videos. These submissions are then voted up or down by other users and organized into communities called "subreddits" based on the subject. "Subreddits" are the core of Reddit, acting as online forums or communities focused on specific topics like technology, gaming, news, or anything else.

78. Your Affiant reviewed the file and in your affiant's opinion, the file is a visual depiction of minor engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256. The file depicts a prepubescent minor girl engaging in the lascivious display of the genitals or pubic area. The file is described below:

- **File / MD5: 7731780f68d5465fcb1012ccac56c6e3** –An image depicting a prepubescent minor girl, wearing a blue shirt and a pink skirt with no underwear, posing for a picture bent over while exposing her vagina.

79. The file was uploaded on 08-03-2023 to Reddit account "Usual_Technology_645."

80. On September 30, 2023, Snapchat submitted Cybertip report 175292892 to NCMEC advising they had identified the Snapchat username, "jeremiah_wa5087," who uploaded a suspected file of child pornography into his or her Snapchat account.

81. The Cybertip provided the incident type as "Child Pornography (possession, manufacture, and distribution)" and the incident time as 09-30-2023 at 13:29 UTC.

82. The Cybertip also provided the email address is feddyjeddy9889@gmail.com and a date of birth as 09-08-1989.

83. As part of the Cybertip, Snapchat provided the file name of one file that was uploaded into this account.

84. The file was uploaded on 09-30-2023 to Snapchat account "jeremiah_wa5087", however the file was not provided to NCMEC, but NCMEC labeled the file "Apparent Child Pornography" based of a "Hash Match [5]."

[5] Hash Matching or Hashing is a technique where a hash value (a unique string of characters that represents digital content, like an image or video) is created for a piece of data, and then that hash value is compared to a hash database of other known values. NCMEC utilizes hash matching to

85. Your affiant advises the email provided by **WALTERS**, during his interview with the NCCPD Detective, "feddyjeddy89@hotmail.com" was identical to the email provided by NCMEC for Cybertip 95489916, 122266818, and 169072158.

86. Your affiant advises the email provided by the WITNESS for **WALTERS**, "feddyjeddy9889@gmail.com" was identical to the email provided by NCMEC for Cybertip 175292892. The Cybertip also provided the username "jeremiah_wa5087" and date of birth "09-08-1989." The first name of **WALTERS** is "Jeremiah," and the date of birth provided by Snapchat is identical to **WALTERS'** date of birth.

H. FBI Interview of WALTERS – 05/02/2025

87. On May 2, 2025, a post-*Miranda* interview was conducted with WALTERS with Agents of the FBI. During the interview, WALTERS admitted to receiving, possessing and sending videos and images related to child pornography.

88. When discussing various NCMEC Cybertips, previously listed above, WALTERS advised he did recall receiving and sending several files containing child pornography and recalled talking about child pornography online with individuals.

89. WALTERS was shown conversations with other online users discussing child pornography, as well as redacted files of child pornography, from the above listed NCMEC Cybertips. WALTERS recognized the conversations and did recall having the conversations. WALTERS also recalled several of the redacted child pornography files.

90. WALTERS advised he would masturbate when watching child pornography.

---

identify known child pornography by comparing the hash value against a database of hashes from previously identified and confirmed child pornography.

91. WALTERS said there may be child pornography saved on his electronic devices. WALTERS advised his current cell phone, **TARGET DEVICE 1**, may have child pornography on the phone and it sometimes automatically saves when viewing and if it did save, it would save in downloads, files, or photos.

CHARACTERISTICS COMMON TO CONSUMERS OF CHILD PORNOGRAPHY

92. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions about child exploitation investigations, I know there are certain characteristics common to individuals who distribute, receive, possess, or access child pornography ("consumers" of child pornography):

a. Consumers of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies from viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, in other visual media, or in literature describing such activity.

b. Consumers of child pornography may collect sexually explicit or suggestive materials in a variety of media, including in hard copy and electronic format. Individuals who have a sexual interest in children or images of children often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children that they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Consumers of child pornography often retain pictures, videos, digital media, and other documentation of child pornography and child erotica for many years.[6] Such individuals prefer not to be without their child pornography for any prolonged time period.

[6] *See United States v. Morales–Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008) (noting that "customers of child pornography sites do not quickly dispose of their cache"… "[t]his is not a new revelation," and finding that evidence was not stale despite more than three-year gap between acquisition of evidence and acquisition of the warrant); *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, *e.g.*, *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

d. Consumers of child pornography often maintain their digital or electronic child pornography in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis, sometimes in an attempt to destroy evidence and evade law enforcement. Evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and other digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it. Thus, even if **WALTERS** has since deleted the files described above from his devices, traces of their existence can still be found through a specialized forensic examination and can help confirm the appropriate venue in which to bring charges against **WALTERS**.

e. Consumers of child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. Furthermore, individuals who would have knowledge about how to access a hidden and embedded chat site would have gained knowledge of its location through online communication with others of similar interest. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, e-mail, bulletin boards, chat sites, web forums, instant messaging applications, and other similar vehicles of communication.

f. Consumers of child pornography often collect, read, copy, or maintain names, screen names or nicknames, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original medium from which they were derived, in written hardcopy, on computer storage devices, or merely on scraps of paper.

93. Based on my training and experience and the training, and experience of other law enforcement officers with whom I have had discussions about child exploitation investigations, I know that persons engaged in the possession of child erotica are also often

involved in the possession of child pornography. Likewise, persons involved in the possession of child pornography are often involved in the possession of child erotica.

94. Based on my training, knowledge, experience, and conversations with others in law enforcement, I understand that an individual who possesses images and/or videos depicting child pornography on one digital storage device and/or Internet email, or online storage account is likely to possess child pornography on additional digital storage devices and/or Internet email or online storage accounts that he possesses or controls.

95. Based on the information contained herein, I submit that **WALTERS** likely exhibits at least some characteristics common to consumers of child pornography. Specifically, **WALTERS** used the internet to connect with other individuals with a sexual attraction to children and **WALTERS** appeared to have possessed and distributed child pornography with those other individuals.

BACKGROUND ON ELECTRONIC DEVICES AND CHILD PORNOGRAPHY

96. I have had training and experience in the investigation of computer-related crimes, including those involving child pornography. Based on my training and experience, and the training and experience of other law enforcement officers with whom I have had discussions that conduct child exploitation investigations, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable, or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

d. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Google, Yahoo!, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

e. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, *i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, *e.g.*, traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used.

f. Some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence, suspects, or victims. For example, the file data for images stored on a computer may provide geolocation information or information indicating when the file or image was created.

TECHNICAL TERMS

97. Based on my training and experience, I use the following technical terms to convey the following meanings:

i. Cellular telephone: A wireless telephone (also known as a mobile telephone or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

ii. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

iii. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

iv. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the

addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

v. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

vi. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

vii. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

98. Based on my training, experience, and research, your affiant is aware that electronic devices like the **TARGET DEVICES** have capabilities that allow them to serve as cellular telephones, digital cameras, portable media players, GPS navigation devices, and PDAs,

and that they can also access the Internet. In my training and experience, examining data stored on devices of this type in investigations such as the instant investigation can uncover, among other things, evidence of the alleged criminal activity.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

99. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Even when a user deletes information from a device, it can sometimes be recovered with forensics tools. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

100. A thorough search of digital media, such as the TARGET DEVICES, for evidence or instrumentalities of a crime commonly requires a qualified expert to conduct the search in a laboratory or other controlled environment. This is true for the following reason – searching digital media requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover hidden, erased, compressed, encrypted, or password-protected data. Since such data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential in conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

101. Searching for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal

evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment B, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, FBI intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

102. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **TARGET DEVICES** were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the **TARGET DEVICES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information

on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

103. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

LOCATION OF THE TARGET DEVICES

104. The **TARGET DEVICES** are currently located at NCCPD Headquarters at 3601 N. Dupont Highway, New Castle, Delaware. The devices were seized by Law Enforcement from the incident involving **WALTERS** and the WITNESS. In my training and experience, I know that the **TARGET DEVICES** have been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as it was when the **TARGET DEVICES** first came into the possession of law enforcement.

CONCLUSION

105. Based on the information described above, I submit that there is probable cause to believe that evidence, contraband, fruits, and instrumentalities, further described in Attachment B, of violations of Title 18, United States Code, Sections 2252(a)(2) and (a)(4)(b), (b)(1), (b)(2) (distribution and possession of child pornography, and attempt), the **SPECIFIED FEDERAL OFFENSES**, will be found in **TARGET DEVICES 1, 2, 3, 4, 5, 6, 7, 8 and 9,** further described in Attachment A, and therefore respectfully requests that the Court issue search warrants to search the same.

Respectfully submitted,

/s/ Brian Mitchell
Special Agent Brian S. Mitchell
Federal Bureau of Investigation

Sworn to me over the telephone and signed by me pursuant to
Fed. R. Crim. P. 4.1 on this 8th day of July, 2025.

THE HONORABLE ELEANOR G. TENNYSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

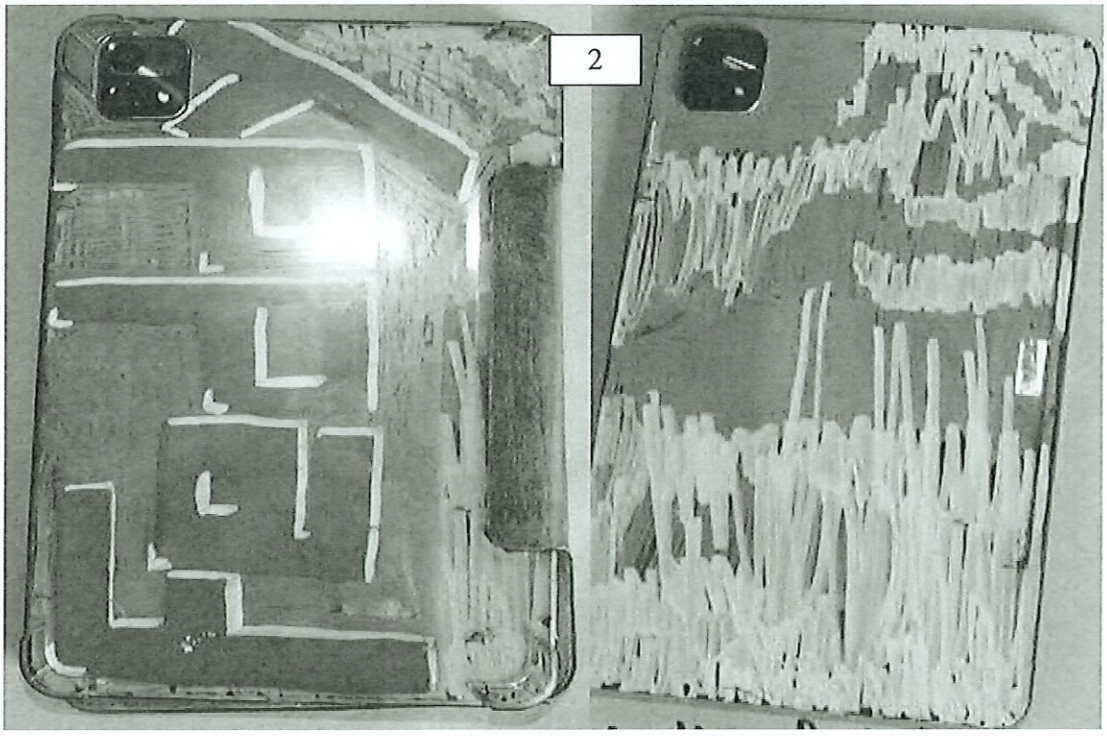
ITEMS TO BE SEARCHED

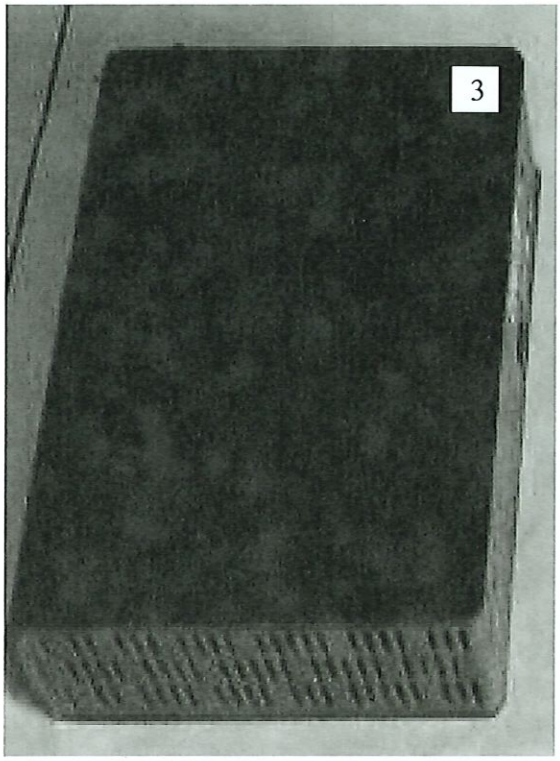
The property to be searched are the following items currently located at New Castle County Police Department:

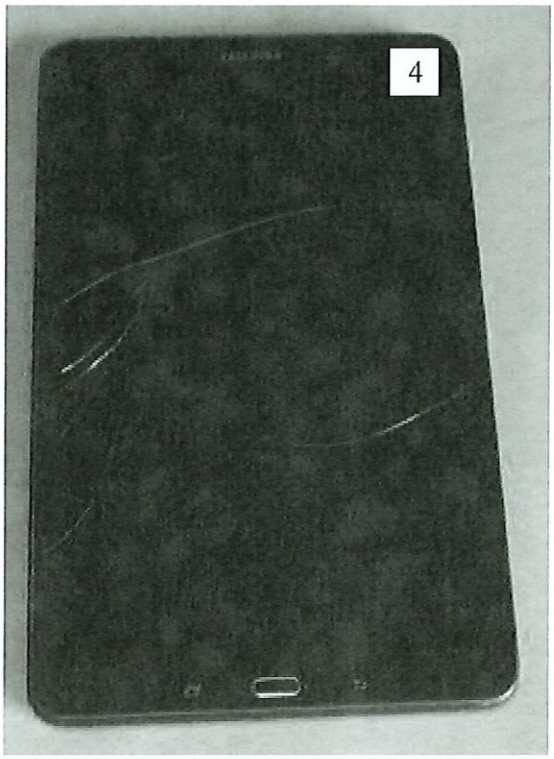
1. Blue Motorola cellphone (cracked upper right portion of screen) – seized from JEREMIAH WALTERS ("**TARGET DEVICE 1**") (Photograph from BWC from NCCPD – Phone currently in a faraday bag at NCCPD)
2. Tablet (Painted purple back in multicolored case with name "Feddy" written on case) – seized from inside leather folder front passenger floorboard of Ford truck ("**TARGET DEVICE 2**")
3. WD My Book Hardrive (Black) – seized from inside backpack front passenger floorboard of Ford truck ("**TARGET DEVICE 3**")
4. Black Samsung tablet (No case), (SN: R52HA1GPF3T) – seized from inside backpack front passenger floorboard of Ford truck ("**TARGET DEVICE 4**")
5. White HP Tablet (Beats label – lower right-hand corner) – seized from inside backpack front passenger floorboard of Ford truck ("**TARGET DEVICE 5**")
6. Black Toshiba Laptop (SN: XE254740P) – seized from front passenger floorboard of Ford truck ("**TARGET DEVICE 6**")
7. Black Toshiba Laptop (SN: 6C351646Q) – seized from under front passenger seat of Ford truck ("**TARGET DEVICE 7**")
8. Black cellphone marker on back of phone (cracked screen) – provided by WITNESS from RV ("**TARGET DEVICE 8**")
9. Black Schok cellphone (cracked screen) – provided by WITNESS from RV ("**TARGET DEVICE 9**")

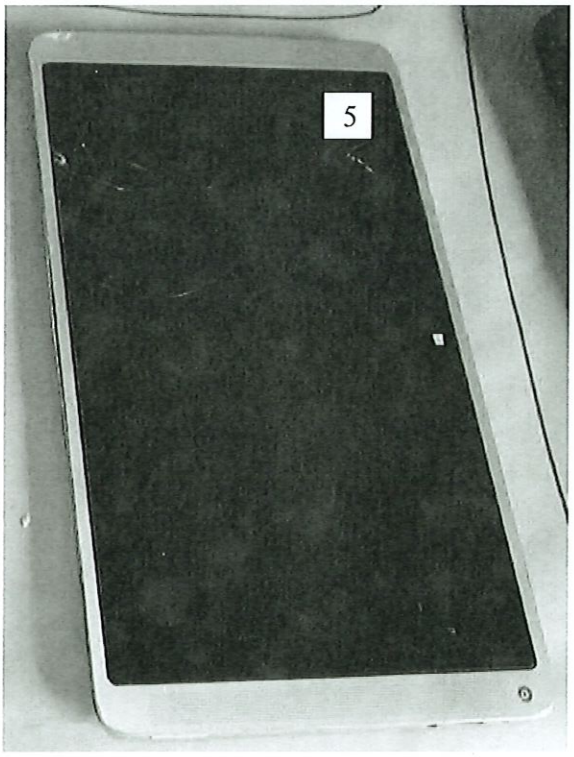
All items (**the "TARGET DEVICES"**) were recovered by Law Enforcement from **WALTERS** during Law Enforcement contact on April 24, 2025. The **TARGET DEVICES** are currently located at the NCCPD Headquarters at 3601 N. Dupont Highway, New Castle, Delaware. Pictures of the "**TARGET DEVICES**" are below:

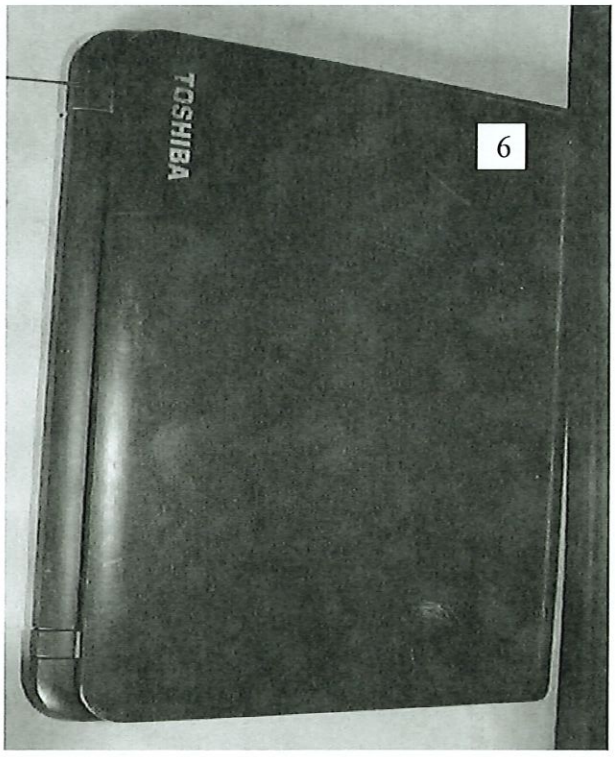

1

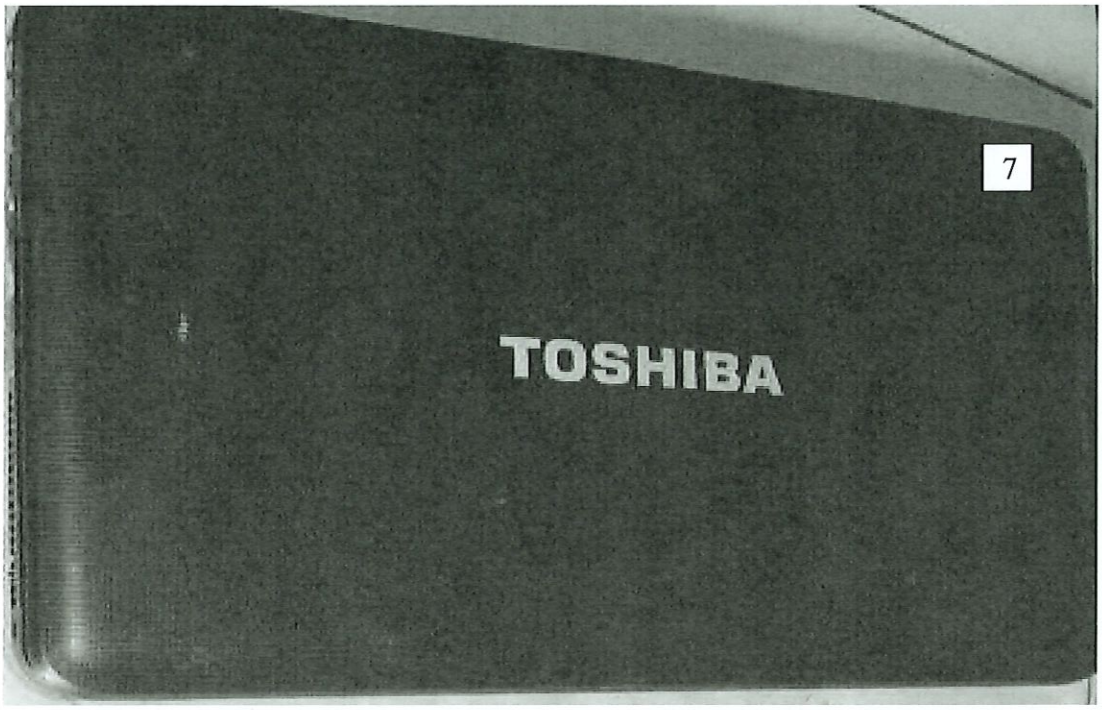

2


3

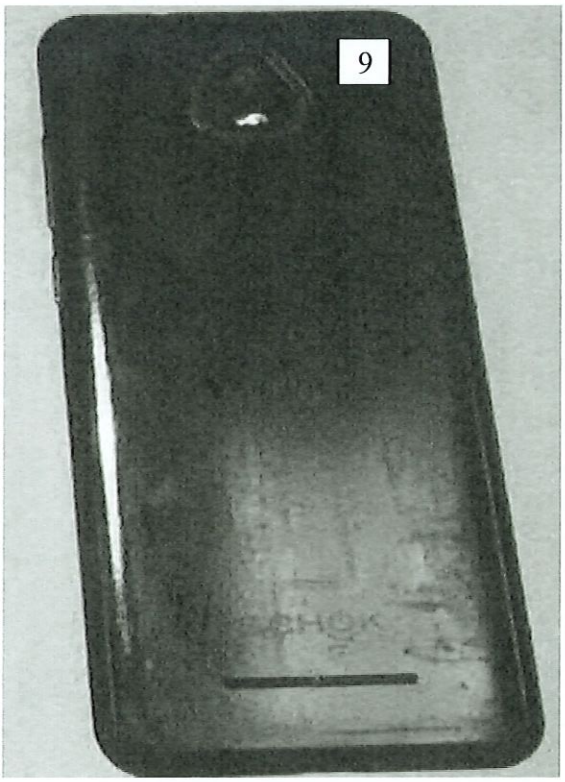

4


5


TOSHIBA
6


7
TOSHIBA


8


9

ATTACHMENT B

INFORMATION TO BE SEIZED

1. All records on the **TARGET DEVICES** described in Attachment A that relate to violations of Title 18, United States Code, Sections 2252(a)(2) and (a)(4)(b), (b)(1), (b)(2) (distribution and possession of child pornography, and attempt), the SPECIFIED FEDERAL OFFENSES listed in the Affidavit, from July 1, 2021 to April 24, 2025, including:

a. The cellular telephone numbers and/or direct connect and/or names and identities, including electronic mail addresses, usernames, and passwords assigned to the devices.

b. Text messages, call history, contact lists, electronic mail messages, chat logs, search history, photos, videos, payment records, and any other documents or information (in whatever form) relating to the distribution and possession of visual depictions of minors engaging in sexually explicit conduct.

c. All visual depictions of minors engaging in sexually explicit conduct, on whatever medium (e.g. digital media, optical media), including but not limited to SIM cards and flash memory cards, also including those in opened or unopened e-mails or text messages.

d. Any information relating to **WALTERS** schedule or travel from July 1, 2021 through April 24, 2025.

e. All bank records, checks, credit card bills, account information, and other financial records, including those from money transfer services such as CashApp.

f. Evidence showing the historic physical locations of the cellular phone.

2. Evidence of user attribution showing who used or owned the **TARGET DEVICES** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the term "records" includes all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of

computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ☑ Original ☐ Duplicate Original

FILED
JUL 08 2025
U.S. DISTRICT COURT
DISTRICT OF DELAWARE

UNITED STATES DISTRICT COURT

for the

District of Delaware

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
3. One WD My Book Hard drive (black), currently located at New Castle County Police Dept., 3601 N. Dupont Hwy, New Castle, DE

Case No. 25- 368M

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of Delaware
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before July 21, 2025 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Duty Magistrate.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 7/8/2025 @ 10:15 am

Judge's signature

City and state: Wilmington, Delaware

Hon. Eleanor G. Tennyson, U.S. Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return		
Case No.: 25-	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title